



BEST AVAILABLE COPY

PATENT
09/801,612

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: : Group Art Unit: 2143
: Examiner: A. M. Lezak
Gerald F. McBrearty et al. : Intellectual Property
Serial No: 09/801,612 : Law Department - 4054
Filed: 03/08/2001 : International Business
Title: PROTECTING CONTENTS : Machines Corporation
OF COMPUTER DATA FILES FROM : 11400 Burnet Road
SUSPECTED INTRUDERS BY : Austin, Texas 78758
RENAMING AND HIDING DATA : Customer No. 32,329
FILES SUBJECTED TO INTRUSION :
Date: 11/23/04 :

DECLARATION UNDER 37 C.F.R. 131

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

I, J. B. Kraft, the attorney herein, declare that:
I am the attorney herein.

Prior to February 5, 2001, I received a copy of International Business Machines Corporation's Invention Disclosure AUS8-2000-1262, entitled: "Self-morphing file to elude hacker capture" which was assigned International Business Machines Corporation (IBM) Attorney Docket No. AUS920000941US1, which is attached hereto as Exhibit A, with its dates customarily blacked out. This disclosure provided the basic disclosure for the present Patent Application.

In due course within my regular workload schedule, after preliminary discussions with the inventors, I commenced the actual written preparation of the present patent application on February 5, 2001 and completed my

UAS920000941US1

PATENT
09/801,612

final draft of the application on February 12, 2001. On that date, the application and the claims therein were substantially in their present form. On or about February 12, 2001, I forwarded the final draft of the present patent application to IBM's IPLaw Department.

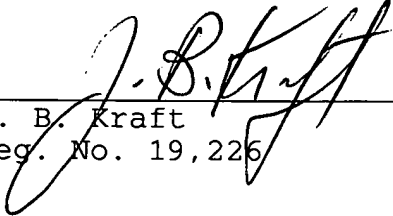
Based partly on my knowledge, and partly upon information and belief, IBM's IPLaw Department proceeded to obtain review by the inventors herein, some minor corrections were made, and the application was filed in the United States Patent and Trademark Office on March 8, 2001, (24 days after my final draft was completed).

Attached hereto and marked Exhibit B are copies pages of my Diary with entries during the period I was working on the present application. The entries indicate that I commenced the writing of the application on February 5, 2001 and that I completed my work on the application on February 12, 2001; the application is initially designated by its Attorney Docket Number: "AUS920000941", and on subsequent entries, by "0941 docket". The entries indicate that I continuously diligently worked on the application for a total of 49 hours during the period.

I hereby declare that all statements made herein are of my own knowledge and are true and that all statements made on information and belief are believed to be true; and

PATENT
09/801,612

further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.



J. B. Kraft
Reg. No. 19,226

Date: 11/23/04

U 0592000 0941 US/
EXHIBIT A SN09801,612



Disclosure AUS8-2000-1262

Created By: Johnny Shieh Created On: 09/28/2000 12:23:57 PM

Last Modified By: Johnny Shieh Last Modified On: 09/29/2000 08:07:48 AM

*** IBM Confidential ***

Required fields are marked with the asterisk (*) and must be filled in to complete the form.

Summary

Status	Under Evaluation
Processing Location	AUS
Functional Area	BP - SD - DEVELOPMENT AIX/6000 (H. Armitage)
Attorney/Patent Professional	Volel Emile/Austin/IBM
IDT Team	Rick Poston/Austin/IBM; Gerald McBrearty/Austin/IBM; Kenneth Banning/Austin/IBM; Johnny Shieh/Austin/IBM; Thomas Weaver/Austin/IBM; Kim Tran/Austin/IBM; Arthur Tysor/Austin/IBM; Deanna Brown/Austin/IBM; Alan MacKay/Austin/IBM; Mark-David McLaughlin/Austin/IBM
Submitted Date	09/28/2000 12:37:04 PM
Owning Division	SD
PVT Score	To calculate a PVT score, use the 'Calculate PVT' button.
Incentive Program	
Lab	
Technology Code	

Inventors with Lotus Notes IDs

Inventors: Johnny Shieh/Austin/IBM, Gerald McBrearty/Austin/IBM, Shawn Mullen/Austin/IBM, Michael W Wortman/Austin/IBM@IBMUS

Inventor Name > denotes primary contact	Inventor Serial	Div/Dept	Manager Serial	Manager Name
Shieh, J.M. (Johnny)	549539	7T/B9RS	462923	Munillo, Jessica Kelley
McBrearty, G.F. (Gerald)	614334	7T/E92S	259952	Marks, John J.
Mullen, S.P. (Shawn)	549238	7T/F13S	579637	Ruyle, R.R. (Robert)
Wortman, Michael W.	355548	7T/4CJS	591475	Freitas, D.K. (Kaana)

Inventors without Lotus Notes IDs

IDT Selection

IDT Team: Rick Poston/Austin/IBM Gerald McBrearty/Austin/IBM Kenneth Banning/Austin/IBM Johnny Shieh/Austin/IBM Thomas Weaver/Austin/IBM Kim Tran/Austin/IBM Arthur Tysor/Austin/IBM Deanna Brown/Austin/IBM Alan MacKay/Austin/IBM Mark-David McLaughlin/Austin/IBM	Attorney/Patent Professional: Volel Emile/Austin/IBM
---	--

Response Due to IP&L : 10/29/2000

Main Idea

*Title of disclosure (in English)

Self-morphing file to elude hacker capture.

*Idea of disclosure

1. Describe your invention, stating the problem solved (if appropriate), and indicating the advantages of using the invention.

This is typical of what happens when a hacker breaks into a supposedly secure site:

- a) break in via a security hole
- b) log into the machine as root
- c) try reading or trashing files
- d) if a file has kerberos protection, download the file to local machine for cracking at a later time.

Table

This disclosure proposes a file attribute that allows it to:

- 1) rename itself
- 2) move itself to another directory
- 3) change it's own sum check by adding a few junk bits to the end of the file
- 4) notifying the owner of the kerberos protected file (in a secret method) about the changes.

So what would happen is that if a person broke into a machine as root, they might try to read the contents of the file "customer_credit_cards". This will fail because, although the person is root, they are not kerberos authenticated. The read fails, and then internal logic within the filesystem detects that this file has a auto-rename-move attribute in it. It then renames the file "dow_jones_avg", appends a small file (for example /etc/motd) to the end of the file, then moves it over to /usr. The filesystem then creates a log of this change and places this record in a secret location in a secret filename (for example /usr/bin/x.html). By doing this, the hacker will be fooled into still looking for the file "customer_credit_cards" and/or looking for the same file by scanning for all files with the same original sumcheck. But, they will fail because the file has been moved, renamed, and the sumcheck harmlessly changed with a static file added to it.

An alternative to this idea is to move/change/rename the file, but leave a bogus copy of the file "customer_credit_cards", possibly with counterfeit credit card numbers (no real customers) that can help the authorities track down the users of the "stolen" credit card numbers.

2. How does the invention solve the problem or achieve an advantage,(a description of "the invention", including figures inline as appropriate)?

This idea will continually hide the file and try to jump one step ahead of people probing a system looking for a file. It does not delete the file and notifies the kerberos owner of the file of the history of the attacks on the file and the location of the file as it goes into hiding.

3. If the same advantage or problem has been identified by others (inside/outside IBM), how have those others solved it and does your solution differ and why is it better?

Have not seen this type of evasion before.

4. If the invention is implemented in a product or prototype, include technical details, purpose, disclosure details to others and the date of that implementation.
not currently implemented.

*Critical Questions (Questions 1 - 7 must be answered)

monday 5 february

6th week
36-328

FEBRUARY 2001
M Tu W Th F Sa S
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28

8
30
9
30
10
30
11
30
12
30
1
30
2
30
3
30
4
30
5
30
6
30
7
30
8
30
9

EXHIBIT B

SN 09/801612

19981238 N/A - 3 hours

19981238 (H) AK (NO)

tuesday 6 february

MARCH 2001
M Tu W Th F Sa S
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31

6th week
37-328

8
30
9
30
10
30
11
30
12
30
1
30
2
30
3
30
4
30
5
30
6
30
7
30
8
30
9

19981241

docket

Boers

wednesday 7 february

6th week
38-327

FEBRUARY 2001
M Tu W Th F Sa S
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28

AT9-98-238

N/A due

~~0941~~ 0941 docket
Shores

thursday 8 february

6th week
39-328

MARCH 2001
M Tu W Th F Sa S
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31

0941 docket
Shores

friday 9 february

8th week
40-325

FEBRUARY 2001
M T W Th F Sa S
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28

8 30 9 30 10 30 11 30 12 30 1 30 2 30 3 30 4 30 5 30 6 30 7 30 8 30 9 30

AT998012

N/A

AT998012 (wo AF)

0941 docket

Starr

saturday 10 february

8th week
41-324

MARCH 2001
M T W Th F Sa S
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31

8 30 9 30 10 30 11 30 12 30 1 30 2 30 3 30 4 30 5 30 6 30 7 30 8 30 9 30

0941

docket 4 hours

sunday 11 february

8th week
42-323

FEBRUARY 2001
M T W Th F Sa S
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28

8

30

9

30

10

30

11

30

12

30

1

30

2

30

3

30

4

30

5

30

6

30

7

30

8

30

9

monday 12 february

MARCH 2001

M T W Th F Sa S
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31

7th week
43-322

8

30

9

30

10

30

11

30

12

30

1

30

2

30

3

30

4

30

5

30

6

30

7

30

8

30

9

0941

check

Shous



PATENT
09/801,612

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: : Group Art Unit: 2143
: Examiner: A. M. Lezak
Gerald F. McBrearty et al. : Intellectual Property
Serial No: 09/801,612 : Law Department - 4054
Filed: 03/08/2001 : International Business
Title: PROTECTING CONTENTS : Machines Corporation
OF COMPUTER DATA FILES FROM : 11400 Burnet Road
SUSPECTED INTRUDERS BY : Austin, Texas 78758
RENAMING AND HIDING DATA : Customer No. 32,329
FILES SUBJECTED TO INTRUSION :
Date: _____ :

DECLARATION UNDER 37 C.F.R. 131

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

I, Gerald F. McBrearty declare that:

I am one of the inventors and applicants herein.

I have read the Declaration of our Attorney J. B. Kraft, filed herewith.

Based upon information and belief and knowledge, my Declaration made herein and the Declaration of J. B. Kraft, attorney establish the existence of the written concept from before the February 16, 2001 filing date of published US Patent Application: 20020038296, N. H. Margolus et al., and due diligence to the March 6, 2001 filing date of the present application.

I have reviewed the independent claims in the present application, and declare prior to February 16, 2001 the inventors herein had completed the full concept of the

AUS920000941US1

1

PATENT

09/801.612

combination of elements set forth in these claims and had recorded the same in the written disclosure. Exhibit "A" of the Declaration of J. B. Kraft; and prior to February 16, 2001, the present invention was fully disclosed in the final draft of this application submitted to IBM's IPLaw Department on February 12, 2001.

I hereby declare that all statements made herein are of my own knowledge and are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.


Gerald F. McBreartyDate: 11-23-2004

AUS920000941US1

2

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.